

Access Control and Privacy Policies (6)

Email: christian.urban at kcl.ac.uk

Office: S1.27 (1st floor Strand Building)

Slides: KEATS (also homework is there)

Access Control Logic

Formulas

$F ::=$ true
| false
| $F \wedge F$
| $F \vee F$
| $F \Rightarrow F$
| $p(t_1, \dots, t_n)$
| **P says F**

“saying predicate”

Judgements

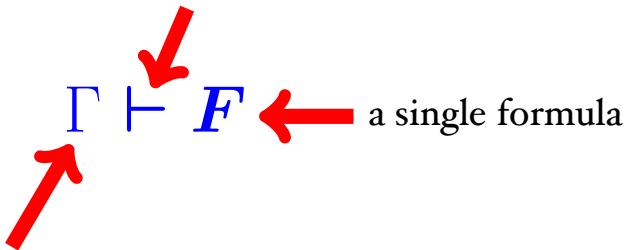
$\Gamma \vdash F$

Judgements

$\Gamma \vdash F$

Judgements

entails sign



Gamma

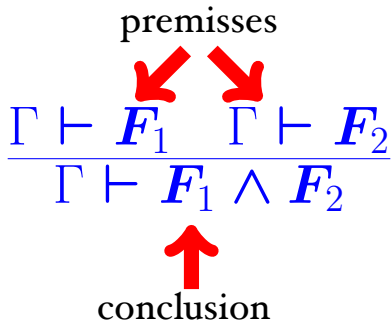
stands for a collection of formulas
("assumptions")

Inference Rules

premisses

$$\frac{\Gamma \vdash F_1 \quad \Gamma \vdash F_2}{\Gamma \vdash F_1 \wedge F_2}$$

conclusion



Inference Rules

premisses

$$\frac{\Gamma \vdash F_1 \quad \Gamma \vdash F_2}{\Gamma \vdash F_1 \wedge F_2}$$

conclusion

P says $F \vdash Q$ says $F \wedge P$ says G

Inference Rules

premisses

$$\frac{\Gamma \vdash F_1 \quad \Gamma \vdash F_2}{\Gamma \vdash F_1 \wedge F_2}$$

conclusion

$$\underbrace{P \text{ says } F}_{\Gamma} \vdash \underbrace{Q \text{ says } F}_{F_1} \wedge \underbrace{P \text{ says } G}_{F_2}$$

Inference Rules

$$\overline{\Gamma, F \vdash F}$$

$$\frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2}$$

$$\frac{F_1, \Gamma \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2}$$

$$\frac{\Gamma \vdash F}{\Gamma \vdash P \text{ says } F}$$

$$\frac{\Gamma \vdash P \text{ says } (F_1 \Rightarrow F_2) \quad \Gamma \vdash P \text{ says } F_1}{\Gamma \vdash P \text{ says } F_2}$$

Sending Messages

- Alice sends a message m

Alice says m

Sending Messages

- Alice sends a message m

Alice says m

- Alice sends an encrypted message m with key K

$(\{m\}_K \stackrel{\text{def}}{=} K \Rightarrow m)$

Alice says $\{m\}_K$

Sending Messages

- Alice sends a message m

Alice says m

- Alice sends an encrypted message m with key K

$(\{m\}_K \stackrel{\text{def}}{=} K \Rightarrow m)$

Alice says $\{m\}_K$

- Decryption of Alice's message

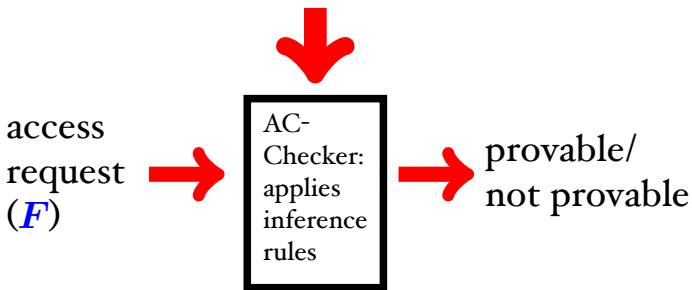
$$\frac{\Gamma \vdash \text{Alice says } \{m\}_K \quad \Gamma \vdash \text{Alice says } K}{\Gamma \vdash \text{Alice says } m}$$

Proofs

$$\frac{\frac{\vdots}{\text{---}} \quad \frac{\vdots \quad \vdots}{\text{---}}}{\text{---}} \quad \vdots}{\Gamma \vdash F}$$

The Access Control Problem

Access Policy (Γ)



Proofs

$\frac{}{\top}$ axiom

$\frac{\top}{\top}$

$\frac{\top \quad \top}{\top}$



goal

start

Sudoku

ROWS

	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

columns

- 1 **Row-Column:** each cell, must contain exactly one number
- 2 **Row-Number:** each row must contain each number exactly once
- 3 **Column-Number:** each column must contain each number exactly once
- 4 **Box-Number:** each box must contain each number exactly once

Solving Sudokus

			7				5	8
5	6	2	I	8	7	9	3	
					I			
						8	I	
			3	7	6			
9	6							
		5		3				
		4		2	I	8	3	
8	7				3			

single position rules

{1..9} - {4} in one row
4 in empty position

Solving Sudokus

			7				5	8
5	6	2	I	8	7	9	3	
					I			
						8	I	
			3	7	6			
9	6							
		5	3					
		4	2	I	8	3		
8	7				3			

single position rules

{1..9} - {4} in one row
4 in empty position

{1..9} - {x} in one column
x in empty position

{1..9} - {x} in one box
x in empty position

Solving Sudokus

			7			2	5	8
	5	6	2	I	8	7	9	3
						I	2	2
							8	I
			3	7	6			
9	6							
		5		3				
		4		2	I	8	3	
8	7				3			

candidate rules

$X - \{x\}$ in one box $X \subseteq \{1..9\}$
 x candidate in empty positions

Solving Sudokus

			7			2	5	8
4	5	6	2	1	8	7	9	3
						1	2	2
							8	1
			3	7	6			
9	6							
		5	3					
		4	2	1	8	3		
8	7				3			

$\{1..9\} - \{4\}$ in one row
4 in empty position





$X - \{2\}$ in one box $X \subseteq \{1..9\}$
2 candidate in empty positions



Solving Sudokus

			7			2	5	8
4	5	6	2	1	8	7	9	3
						1	2	2
							8	1
			3	7	6			
9	6							
		5	3					
		4	2	1	8	3		
8	7				3			

$\{1..9\} - \{4\}$ in one row 
4 in empty position

$X - \{2\}$ in one box $X \subseteq \{1, 3, 7, 8, 9\}$ 
2 candidate in empty positions

Solving Sudokus

			7				5	8
	5	6	2	I	8	7	9	3
						I		
							8	I
			3	7	6			
9	6							2
		5		3				
		4		2	I	8	3	
8	7				3			

$X - \{2\}$ in one box $X \subseteq \{1..9\}$
2 candidate



Sudoku

Are there sudokus that cannot be solved?

Sudoku

Are there sudokus that cannot be solved?

I	2	3	4	5	6	7	8	
								2
								3
								4
								5
								6
								7
								8
								9

Sometimes no rules apply at all....unsolvable sudoku.

Example Proof

?

P says $F_1 \wedge Q$ says $F_2 \vdash Q$ says $F_2 \wedge P$ says F_1

Example Proof

We have (by axiom)

$$(I) \quad P \text{ says } F_1 \wedge Q \text{ says } F_2 \vdash P \text{ says } F_1 \wedge Q \text{ says } F_2$$

From (I) we get

$$(2) \quad P \text{ says } F_1 \wedge Q \text{ says } F_2 \vdash P \text{ says } F_1$$

$$(3) \quad P \text{ says } F_1 \wedge Q \text{ says } F_2 \vdash Q \text{ says } F_2$$

From (3) and (2) we get

$$P \text{ says } F_1 \wedge Q \text{ says } F_2 \vdash Q \text{ says } F_2 \wedge P \text{ says } F_1$$

Done.

Other Direction

We want to prove

$$P \text{ says } F_1 \wedge Q \text{ says } F_2 \vdash Q \text{ says } F_2 \wedge P \text{ says } F_1$$

We better be able to prove:

- (1) $P \text{ says } F_1 \wedge Q \text{ says } F_2 \vdash Q \text{ says } F_2$
- (2) $P \text{ says } F_1 \wedge Q \text{ says } F_2 \vdash P \text{ says } F_1$

For (1): If we can prove

$$P \text{ says } F_1 \wedge Q \text{ says } F_2 \vdash Q \text{ says } F_2 \wedge P \text{ says } F_1$$

then (1) is fine. Similarly for (2).

I want to prove

$\Gamma \vdash \text{del_file}$

I want to prove

$$\Gamma \vdash \text{del_file}$$

There is an inference rule

$$\frac{\Gamma \vdash \mathbf{F}}{\Gamma \vdash \mathbf{P \text{ says } F}}$$

I want to prove

$$\Gamma \vdash \text{del_file}$$

There is an inference rule

$$\frac{\Gamma \vdash F}{\Gamma \vdash P \text{ says } F}$$

So I can derive $\Gamma \vdash \text{Alice says del_file}$.

I want to prove

$$\Gamma \vdash \text{del_file}$$

There is an inference rule

$$\frac{\Gamma \vdash F}{\Gamma \vdash P \text{ says } F}$$

So I can derive $\Gamma \vdash \text{Alice says del_file}$.

Γ contains already $\text{Alice says del_file}$.

So I can use the rule

$$\overline{\Gamma, F \vdash F}$$

Done. Qed.

I want to prove

$$\Gamma \vdash \text{del_file}$$

There is an inference rule

$$\frac{\Gamma \vdash F}{\Gamma \vdash P \text{ says } F}$$

So I can derive $\Gamma \vdash \text{Alice says del_file}$.

Γ contains already $\text{Alice says del_file}$.

So I can use the rule

$$\overline{\Gamma, F \vdash F}$$

What is wrong with this?

Done. Qed.

Program

How to prove $\Gamma \vdash F$?

$$\overline{\Gamma, F \vdash F}$$

$$\frac{F_1, \Gamma \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2}$$

$$\frac{\Gamma \vdash \mathbf{F}}{\Gamma \vdash \mathbf{P} \text{ says } \mathbf{F}}$$

$$\frac{\Gamma \vdash \mathbf{F}_1}{\Gamma \vdash \mathbf{F}_1 \vee \mathbf{F}_2}$$

$$\frac{\Gamma \vdash \mathbf{F}_2}{\Gamma \vdash \mathbf{F}_1 \vee \mathbf{F}_2}$$

$$\frac{\Gamma \vdash \mathbf{F}_1 \quad \Gamma \vdash \mathbf{F}_2}{\Gamma \vdash \mathbf{F}_1 \wedge \mathbf{F}_2}$$

Program: prove2

I want to prove $\Gamma \vdash \text{Pred}$

Program: prove2

I want to prove $\Gamma \vdash \text{Pred}$

- I found that Γ contains the assumption $F_1 \Rightarrow F_2$

Program: prove2

I want to prove $\Gamma \vdash \text{Pred}$

- 1 I found that Γ contains the assumption $F_1 \Rightarrow F_2$
- 2 If I can prove $\Gamma \vdash F_1$,

Program: prove2

I want to prove $\Gamma \vdash \text{Pred}$

- 1 I found that Γ contains the assumption $F_1 \Rightarrow F_2$
- 2 If I can prove $\Gamma \vdash F_1$, then I can prove
 $\Gamma \vdash F_2$

$$\frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2}$$

Program: prove2

I want to prove $\Gamma \vdash \text{Pred}$

- 1 I found that Γ contains the assumption $F_1 \Rightarrow F_2$
- 2 If I can prove $\Gamma \vdash F_1$, then I can prove
 $\Gamma \vdash F_2$
- 3 So I am able to try to prove $\Gamma \vdash \text{Pred}$ with the additional assumption F_2 .

$F_2, \Gamma \vdash \text{Pred}$

Recall the following scenario:

- If **Admin** says that **file** should be deleted, then this file must be deleted.
- **Admin** trusts **Bob** to decide whether **file** should be deleted.
- **Bob** wants to delete **file**.

$(\text{Admin says del_file}) \Rightarrow \text{del_file},$

$\Gamma = (\text{Admin says } ((\text{Bob says del_file}) \Rightarrow \text{del_file})),$
 Bob says del_file

$\Gamma \vdash \text{del_file}$

- P is entitled to do F

P controls $F \stackrel{\text{def}}{=} (P \text{ says } F) \Rightarrow F$

$$\frac{\Gamma \vdash P \text{ controls } F \quad \Gamma \vdash P \text{ says } F}{\Gamma \vdash F}$$

Trusted Third Party

Simple protocol for establishing a secure connection via a mutually trusted 3rd party (server):

Message 1 $A \rightarrow S : A, B$

Message 2 $S \rightarrow A : \{K_{AB}\}_{K_{AS}}$ and $\{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$

Message 3 $A \rightarrow B : \{K_{AB}\}_{K_{BS}}$

Message 4 $A \rightarrow B : \{m\}_{K_{AB}}$

Sending Rule

$$\frac{\Gamma \vdash P \text{ says } F \quad \Gamma \vdash P \text{ sends } Q : F}{\Gamma \vdash Q \text{ says } F}$$

Sending Rule

$$\frac{\Gamma \vdash P \text{ says } F \quad \Gamma \vdash P \text{ sends } Q : F}{\Gamma \vdash Q \text{ says } F}$$

$$P \text{ sends } Q : F \stackrel{\text{def}}{=} (P \text{ says } F) \Rightarrow (Q \text{ says } F)$$

Trusted Third Party

A sends S : $\text{Connect}(A, B)$

S says ($\text{Connect}(A, B) \Rightarrow$

$$\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}})$$

S sends A : $\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$

A sends B : $\{K_{AB}\}_{K_{BS}}$

A sends B : $\{m\}_{K_{AB}}$

Trusted Third Party

A sends S : $\text{Connect}(A, B)$

S says $(\text{Connect}(A, B) \Rightarrow$

$$\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}})$$

S sends A : $\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$

A sends B : $\{K_{AB}\}_{K_{BS}}$

A sends B : $\{m\}_{K_{AB}}$

$\Gamma \vdash B$ says m ?

Public/Private Keys

- Bob has a private and public key: K_{Bob}^{pub} , K_{Bob}^{priv}

$$\frac{\Gamma \vdash \text{Alice says } \{m\}_{K_{Bob}^{pub}} \quad \Gamma \vdash K_{Bob}^{priv}}{\Gamma \vdash \text{Alice says } m}$$

Public/Private Keys

- Bob has a private and public key: K_{Bob}^{pub} , K_{Bob}^{priv}

$$\frac{\Gamma \vdash \text{Alice says } \{m\}_{K_{Bob}^{pub}} \quad \Gamma \vdash K_{Bob}^{priv}}{\Gamma \vdash \text{Alice says } m}$$

- this is **not** a derived rule!

Security Levels

- Top secret (*TS*)
- Secret (*S*)
- Public (*P*)

$$\text{slev}(P) < \text{slev}(S) < \text{slev}(TS)$$

Security Levels

- Top secret (*TS*)
- Secret (*S*)
- Public (*P*)

$$\text{slev}(P) < \text{slev}(S) < \text{slev}(TS)$$

- Bob has a clearance for “secret”
- Bob can read documents that are public or secret, but not top secret

Reading a File

Bob controls Permitted (File, read)

Bob says Permitted (File, read)

Permitted (File, read)

Reading a File

$slev(\text{File}) < slev(\text{Bob}) \Rightarrow$

Bob controls Permitted (File, read)

Bob says Permitted (File, read)

$slev(\text{File}) < slev(\text{Bob})$

Permitted (File, read)

Reading a File

$slev(\text{File}) < slev(\text{Bob}) \Rightarrow$

Bob controls Permitted (File, read)

Bob says Permitted (File, read)

$slev(\text{File}) = P$

$slev(\text{Bob}) = S$

$slev(P) < slev(S)$

Permitted (File, read)

Substitution Rule

$$\frac{\Gamma \vdash \mathit{slev}(P) = l_1 \quad \Gamma \vdash \mathit{slev}(Q) = l_2 \quad \Gamma \vdash l_1 < l_2}{\Gamma \vdash \mathit{slev}(P) < \mathit{slev}(Q)}$$

Substitution Rule

$$\frac{\Gamma \vdash \mathit{slev}(P) = l_1 \quad \Gamma \vdash \mathit{slev}(Q) = l_2 \quad \Gamma \vdash l_1 < l_2}{\Gamma \vdash \mathit{slev}(P) < \mathit{slev}(Q)}$$

- $\mathit{slev}(\text{Bob}) = S$
- $\mathit{slev}(\text{File}) = P$
- $\mathit{slev}(P) < \mathit{slev}(S)$

Reading a File

$slev(\text{File}) < slev(\text{Bob}) \Rightarrow$

Bob controls Permitted (File, read)

Bob says Permitted (File, read)

$slev(\text{File}) = P$

$slev(\text{Bob}) = TS$

?

Permitted (File, read)

Reading a File

$slev(\text{File}) < slev(\text{Bob}) \Rightarrow$

Bob controls Permitted (File, read)

Bob says Permitted (File, read)

$slev(\text{File}) = P$

$slev(\text{Bob}) = TS$

$slev(P) < slev(S)$

$slev(S) < slev(TS)$

Permitted (File, read)

Transitivity Rule

$$\frac{\Gamma \vdash l_1 < l_2 \quad \Gamma \vdash l_2 < l_3}{\Gamma \vdash l_1 < l_3}$$

- $slev(P) < slev(S)$
- $slev(S) < slev(TS)$
- $slev(P) < slev(TS)$

Reading Files

- Access policy for reading

$\forall f. \text{slev}(f) < \text{slev}(\text{Bob}) \Rightarrow$
Bob controls Permitted (f , read)

Bob says Permitted (File, read)

$\text{slev}(\text{File}) = P$

$\text{slev}(\text{Bob}) = TS$

$\text{slev}(P) < \text{slev}(S)$

$\text{slev}(S) < \text{slev}(TS)$

Permitted (File, read)

Reading Files

- Access policy for reading

$\forall f. \text{slev}(f) \leq \text{slev}(\text{Bob}) \Rightarrow$
Bob controls Permitted (f , read)

Bob says Permitted (File, read)

$\text{slev}(\text{File}) = \text{TS}$

$\text{slev}(\text{Bob}) = \text{TS}$

$\text{slev}(P) < \text{slev}(S)$

$\text{slev}(S) < \text{slev}(\text{TS})$

Permitted (File, read)

Writing Files

- Access policy for writing

$\forall f. \text{slev}(\text{Bob}) \leq \text{slev}(f) \Rightarrow$
Bob controls Permitted (f , write)

Bob says Permitted (File, write)

$\text{slev}(\text{File}) = TS$

$\text{slev}(\text{Bob}) = S$

$\text{slev}(P) < \text{slev}(S)$

$\text{slev}(S) < \text{slev}(TS)$

Permitted (File, write)